UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,515	07/25/2003	Lee E. Cannon	IGT1P551/P000834-001	3255

79646 7590 11/13/2009

Weaver Austin Villeneuve & Sampson LLP - IGT
Attn: IGT
P.O. Box 70250
Oakland, CA 94612-0250

EXAMINER	
HOEL, MATTHEW D	

ART UNIT	PAPER NUMBER
3714	

NOTIFICATION DATE	DELIVERY MODE
11/13/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@wavsip.com

Office Action Summary	Application No.	Applicant(s)	
	10/627,515	CANNON, LEE E.	
	Examiner	Art Unit	
	Matthew D. Hoel	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *49-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *49-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. Claims 49 to 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martinek, et al. (U.S. pre-grant publication 2003/0130032 A1) in view of Arnold (EPO publication 0 661 675 A2, application 94117809.7, entered as FPL 10-27-2008).

4. As to Claims 49 and 54: Martinek in Martinek discloses all of the limitations of Claims 49 and 54, but lacks specificity as to comparing first and second gaming data from first and second respective gaming organizations in the same embodiment. Martinek in Paras. 83 and 90 teaches a first gaming organization being the Nevada Gaming Regulation Commission, a regulatory agency. Para. 83 of Martinek teaches a second gaming organization being the game manufacturer or designer. Fig. 4 of Martinek teaches decrypting a message digest created from a loadable data set via one public key 238 and its corresponding decryption program 230 and decrypting a signature via another public key 234 and its corresponding decryption program 232 (Fig. 4; Para. 81). Martinek in Fig. 3 teaches taking a loadable data set 212 and creating a

message digest 214 and signature 220 via a public/private key pair 218 (Paras. 79 & 80). Martinek teaches a gaming apparatus (Abst.). There is a display unit (108, Fig. 1); a value input device (104 & 105, Fig. 1); a controller operatively coupled to said display unit and said value input device, said controller comprising a processor and a memory operatively coupled to said processor (Fig. 5) and having first encrypted gaming data stored in the memory (message digest 228, Fig. 4, to be decrypted with decryption program 230) and second encrypted gaming data stored in the memory (signature 240, Fig. 4, to be decrypted with decryption program 231) , said first encrypted gaming data having been generated by encrypting gaming data utilizing an encryption key of a first gaming organization and said second encrypted gaming data having been generated by encrypting gaming data utilizing an encryption key of a second gaming organization, said controller being programmed to retrieve said first encrypted gaming data from the memory (228, Fig. 4, Para. 81);

said controller being programmed to decrypt said first encrypted gaming data (decryption program 230, Fig. 4, decrypting message digest 228) utilizing an encryption key of said first gaming organization to form first decrypted gaming data;

said controller being programmed to retrieve said second encrypted gaming data from the memory (240, Fig. 4, Para. 81);

said controller being programmed to decrypt said second encrypted gaming data (decryption program 232, Fig. 4, decrypting signature 240) utilizing an encryption key of said second gaming organization to form second decrypted gaming data; and

said controller being programmed to determine whether said first decrypted gaming

data is identical to said second decrypted gaming data (comparing step 236, Fig. 4, Para. 81). Martinek teaches enabling a game play operation on the gaming apparatus upon determining that the first encrypted gaming data is identical to the second encrypted gaming data. Para. 73: "The computerized game controller also executes game code, which may be loaded into memory 203 from either a mass storage device 205 such as a hard disc drive, or nonvolatile memory 204 such as flash memory or EPROM memory before execution. In some embodiments, the computerized game controller 201 loads encryption functions into memory 203, and those functions are *subsequently executed* to securely load other gaming system data from the mass storage device 205." (emphasis added). The system also prevents data from subsequently loading if it cannot be authenticated or from subsequently running if it cannot be authenticated (Para. 80). The determination of the first (decryption step 232) and second encrypted data sets (decryption step 230) being the same (comparison step 236) is conducted in Fig. 4 (Para. 81). Martinek teaches a gaming regulatory authority being distinct from the entity that wrote the gaming software (Para. 26, digitally signed by gaming authorities; technique described in Paras. 61, 65; regulators and manufacturers have their own signatures, Paras. 83, 89, & 90). Fig. 3 of Martinek teaches the public/private key pare 218 stored in a controller (Paras. 79 & 80; also, Fig. 10, Paras. 104 & 105). Martinek teaches receiving value from a player via a value device, receiving input from a player via an input device, generating an output of the casino game, and displaying the output (Fig. 1, Para. 67). What Martinek lacks is first encrypting gaming data with a first key from a first gaming organization and a second

key from a second organization and decrypting the gaming data with the first and second keys from the first and second gaming organizations. Martinek does teach first and second gaming organizations, and decrypting first gaming data with one public key and second gaming data with a second public key and then comparing the two gaming data as outlined above. The examiner believes that first encrypting gaming data with a first key from a first gaming organization and a second key from a second organization and decrypting the gaming data with the first and second keys from the first and second gaming organizations is obvious in light of Arnold (Arnold). Regarding decrypting a first data set with a key from a first gaming organization and decrypting a second data set with another key from a second gaming organization and comparing them to see if they are equal, Martinek teaches first and second organizations as being a game developer and a state gaming commission, respectively, as outlined above. Martinek also teaches decrypting two separate data sets with two separate keys, comparing the decrypted data sets, and continuing execution if they are identical as outlined above. The aspect of having the two data sets each being decrypted with respective keys from respective gaming organizations is obvious as outlined by the 103 combination below, and as was last explained in the last office action; all of the elements of the claim were already in Martinek—they simply needed the obviousness teachings of Arnold as outlined below to combine the different teachings (or "embodiments" as there is no clear separation of these two teachings into clearly separate embodiments upon a review of Martinek as Martinek's description moves from one aspect to another). The new limitations do not change the scope of the claim language as they were already addressed above and in

the last office action; they merely paraphrase the previous claims without adding any new limitations. Enabling a game play is not really a substantial new limitation to the claim as it was "anticipated" by the base reference (Martinek). Arnold in Figs. 3, 4, and 5 shows a data set being encrypted with separate keys from separate entities (a user and a supervisor, analogous to a game developer and a Gaming Commission, respectively, of Martinek). Fig. 3, 5:44-6:3 of Arnold describes a data set Xsup being encrypted with a supervisor's session key KS1. Fig. 4, 6:4-19 of Arnold describes the same data set with a user's session key KS2. Fig. 5, 6:20-7:20 of Arnold describes the computation of the decryption value using the supervisor's session key KS1 to recover Xsup and the computation of the decryption value using the user's session key KS2 to recover Xsup. If the two recovered values of Xsup are the same, the desired activity is allowed to continue (steps 65, 69, 71, Fig. 1). The modification the examiner is proposing to make is to apply this parallel encryption and decryption using two separate keys from two organizations to Figs. 3 and 4 of Martinek. The game developer's public/private key pair 218 (Fig. 3) and corresponding encryption program 216 (Fig. 3) and decryption program 230 (Fig. 3) would be used to provide a message digest and signature to the casino operating the gaming machine. The public key of the game developer would be known to the casino and the private key would be only known to the developer. The game developer would also supply the game data loadable set (212 of Fig. 3 and 224 of Fig. 4) to the Gaming Commission, which would sign the loadable data set with its own public/private key pair 218 (Fig. 3) and corresponding encryption program 216 (Fig. 3) and decryption program 232 (Fig. 4), as suggested by Martinek

(Para. 83). The Gaming Commission's public key would be known to the casino and the private key would be known only to the gaming commission. The casino would proceed as described in Fig. 4 of Martinek and decrypt the message digest 228 received from the game developer using the game developer's public key 238 and corresponding decryption program 230 and decrypt the signature using the Gaming Commission's public key 234 and corresponding decryption program 232. If the two values are equal, as in step 236 (Fig. 4 of Martinek, corresponding to step 65 of Arnold's Fig. 5), the gaming activity would be allowed to proceed. Even though the message digest 236 would be received by the casino from the game developer and the signature 240 would be received from the Gaming Commission, they would be the same when decrypted (if authentic), because the were both generated from the same loadable data set (224 of Fig. 4 corresponding to 212 of Fig. 3, Martinek) developed by the gaming manufacturer. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have applied the parallel encryption and decryption of Arnold (Figs. 3 to 5) as described above to the parallel decryption of Martinek (Fig. 4). Both references are analogous in that the supervisor of Arnold corresponds to the Gaming Commission of Martinek and the user of Arnold corresponds to the game developer of Martinek. Both references teach parallel decryption with separate keys and comparing two values to see if they are equivalent as described above. The result is simply a superposition of known encryption techniques. The modification would have the effect and advantage of keeping the Gaming Commission always in the loop, so that casinos would not be able to decrypt and use software

updates from game developers until they have been evaluated and digitally signed by the Gaming Commission (Martinek, Para. 57). Martinek even suggests the decryption being done in the presence of two persons to ensure security (Para. 138). The use of the data set Xsup as taught by Arnold would have an advantage in that the game data set could only be decrypted in the presence of a Gaming Commissioner or delegate representative thereof (the supervisor of Arnold).

5. As to Claims 50 and 55: The display unit of Martinek generates a game display representing poker, blackjack, slots, keno, or bingo (Paras. 7 & 21).

6. As to Claims 51 and 56: Martinek teaches said first gaming data comprising substantially all gaming data necessary to facilitate play of a casino game (self-contained, functional units defining operation of game, Para. 78; see also Fig. 6, Para. 97).

7. As to Claims 52 and 57: Martinek teaches said display unit comprising a video display unit that is capable of generating video images (Para. 7, 67).

8. As to Claim 53: The first organization is a game data authorizing organization being the game developer (Martinek, Para. 89), and the second organization is a gaming regulatory organization being a state gaming commission (Martinek, Para. 89).

9. As to Claim 58: Arnold teaches separate first and second encryption keys as discussed above regarding the independent claims.

Response to Arguments

1. Applicant's arguments filed 07-29-2009 have been fully considered but they are not persuasive. The previous 101 rejections are withdrawn as the claims have been properly amended. Simply put, the applicant's claims are broadly worded and not actually drawn to what the applicant reduced to practice. The claims are not drawn to Fig. 3A in which the gaming information is doubly encrypted, first with a private authoring key, and second with a private regulator key; and to corresponding Fig. 4A, in with the gaming information is doubly decrypted, first with a public regulator key, and second with a public authoring key. Figs. 3B and corresponding 4B do the same thing, except triply encrypting and decrypting the game data with the addition of private and public casino keys for the individual establishment. Nowhere in the claims are double or triple encryption cited. The claims as written are drawn to encrypting and decrypting respective first and second sets of data (copies of the same original gaming data) with keys from respective first and second separate entities, and accepting the gaming data if the two decrypted sets of gaming data are equal. The applicants are claiming *parallel* encryption and decryption, which is much broader than what they reduced to practice in the specification, which is *serial* or superimposed encryption and decryption. Martinek (Fig. 4) and Arnold (Fig. 5) are both drawn to parallel encryption and decryption as discussed in the above rejections and in the discussion below, so the rejections will not be withdrawn. The examiner believes this difference between how broadly the claims are written and what was reduced to practice in the specification are what is causing the different points of view between the examiner and the applicant. The examiner will not

read more into the claims than is actually there. The examiner notes that Fig. 1 of WIPO publication WO 01/06691 A2 (application PCT/US00/19944, entered as FPL on 11-18-2004) discusses double encryption and decryption of gaming data using keys from two separate entities, which appears to be how the applicant intend for his claims to be interpreted. No multiple, serial, or superimposed encryption is cited in the claims at this time. No rejections regarding double or triple encryption have been applied to the claims thus far because multiple encryption has not been claimed thus far.

2. Martinek teaches enabling a game play operation on the gaming apparatus upon determining that the first encrypted gaming data is identical to the second encrypted gaming data. Para. 73: "The computerized game controller also executes game code, which may be loaded into memory 203 from either a mass storage device 205 such as a hard disc drive, or nonvolatile memory 204 such as flash memory or EPROM memory before execution. In some embodiments, the computerized game controller 201 loads encryption functions into memory 203, and those functions are *subsequently executed* to securely load other gaming system data from the mass storage device 205." (emphasis added). The system also prevents data from subsequently loading if it cannot be authenticated or from subsequently running if it cannot be authenticated (Para. 80). The determination of the first (decryption step 232) and second encrypted data sets (decryption step 230) being the same (comparison step 236) is conducted in Fig. 4 (Para. 81). What Martinek lacks is first encrypting gaming data with a first key from a first gaming organization and a second key from a second organization and decrypting the gaming data with the first and second keys from the first and second

gaming organizations. Martinek does teach first and second gaming organizations, and decrypting first gaming data with one public key and second gaming data with a second public key and then comparing the two gaming data as outlined above. The examiner believes that first encrypting gaming data with a first key from a first gaming organization and a second key from a second organization and decrypting the gaming data with the first and second keys from the first and second gaming organizations is obvious in light of Arnold (Arnold). Regarding decrypting a first data set with a key from a first gaming organization and decrypting a second data set with another key from a second gaming organization and comparing them to see if they are equal, Martinek teaches first and second organizations as being a game developer and a state gaming commission, respectively, as outlined above. Martinek also teaches decrypting two separate data sets with two separate keys, comparing the decrypted data sets, and continuing execution if they are identical as outlined above. The aspect of having the two data sets each being decrypted with respective keys from respective gaming organizations is obvious as outlined by the 103 combination below, and as was last explained in the last office action; all of the elements of the claim were already in Martinek—they simply needed the obviousness teachings of Arnold as outlined below to combine the different teachings already present in Martinek(or "embodiments" as there is no clear separation of these two teachings into clearly separate embodiments upon a review of Martinek as Martinek's description moves from one aspect to another). The new limitations do not change the scope of the claim language as they were already addressed above and in the last office action; they merely paraphrase the previous

claims without adding any new limitations. Enabling a game play is not really a substantial new limitation to the claim as it was "anticipated" by the base reference (Martinek). Pages 5 to 11 of the remarks generally characterize the teachings of the references. Fig. 4 and Para. 81 of Martinek teach separate public keys; a review of the Martinek reference does not indicate that having the public keys being from separate gaming organizations such as a game developer and a state gaming commission would render the decryption system inoperable for its intended purpose or alter its mode of operation. In the 103 combination as described above, the game developer would pass the original data set to the gaming commission for evaluation and approval, and the gaming commission would encrypt the data set with its own private signature if the data set met all regulations and was approved. The game developer would, of course, have the original data set as they would be the ones who developed the game. They would sign the data set with their own private signature. The two decrypted data sets, decrypted with the separate public keys (the private keys remaining private) would then be compared and the game would be allowed to proceed if the data sets are identical, indicating that no tampering had taken place. Regarding Arnold, the user and the supervisor, were analogous to the entities of Martinek, being the game developer and the gaming commission, respectively. The supervisor of Arnold has authority over the user in the same manner that the gaming commission of Martinek has authority over the game developer. In both processes, the same set of game data is encrypted with two separate keys, decrypted with two separate keys, and an action is allowed to take place if the two decrypted data sets are identical (Martinek, Fig. 4, Para. 81; Arnold, Fig. 5,

6:20-7:35, esp. 6:33-45, 6:54-7:3, 7:6-10,23-27), so the two processes are clearly analogous. Martinek uses public-private key pairs and Arnold uses session keys. The public-private key pairs of Martinek has the advantage in that the data set can be signed by each entity with a private key that is not divulged, and decrypted with each entity's known public key, so each decrypted data set is positively identified as having been encrypted by the respective party, without each party's private key being divulged. The examiner respectfully disagrees with the applicant as to the claims' condition for allowance.

Conclusion

3. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

4. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew D. Hoel whose telephone number is (571) 272-5961. The examiner can normally be reached on Mon. to Fri., 8:00 A.M. to 4:30 P.M.

6. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Peter Vo can be reached on (571) 272-4690. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

7. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Matthew D. Hoel
Patent Examiner
AU 3714

Peter Vo
Supervisory Patent Examiner
Art Unit 3714

/M. D. H./
Examiner, Art Unit 3714

/Peter D. Vo/
Supervisory Patent Examiner, Art Unit 3714